Codes as modules over skew polynomial rings

Delphine Boucher, Félix Ulmer

Codes as modules over skew polynomial rings

Delphine Boucher [1] and Felix Ulmer [1]

[1]Université de Rennes 1, IRMAR, France; CNRS, UMR 6625, France;
Université européenne de Bretagne, France

June 24, 2009

Abstract

In previous works we considered codes defined as ideals of quotients of non commutative polynomial rings, so called Ore rings of automorphism type. In this paper we consider codes defined as modules over non commutative polynomial rings, removing therefore some of the constraints on the length of the codes defined as ideals. The notion of BCH codes can be extended to this new approach and the codes whose duals are also defined as modules can be characterized. We show that under some restriction, self dual module codes must be constacyclic ideal codes and found two non equivalent Euclidean self-dual $[56, 28, 15]_4$ codes which improve the best previously known distance 14 for self-dual codes of this length over $\mathbb{F}_4$.

1 Coding with skew polynomial rings

Starting from the finite field $\mathbb{F}_q$ and an automorphism θ of $\mathbb{F}_q$, we define a ring structure on the set:

$$R = \mathbb{F}_q[X, \theta] \, = \, \{a_n X^n + \ldots + a_1 X + a_0 \,|\, a_i \in \mathbb{F}_q \text{ and } n \in \mathbb{N}\} \, .$$

The addition in R is defined to be the usual addition of polynomials and the multiplication is defined by the basic rule $X\, a = \theta(a)\, X$ $(a \in \mathbb{F}_q)$ and extended to all elements of R by associativity and distributivity (cf. [1, 7, 8]). The ring R is a left and right Euclidean ring whose left and right ideals are principal [8]. In the following we denote $\mathbb{F}_q^\theta \subset \mathbb{F}_q$ the fixed field of θ.

1.1 Ideal θ-codes

In [4] we defined codes as ideals of quotient rings of R. If $I = (f)$ is a two sided ideal of R, then, in analogy to classical cyclic codes, we associate to an element $a(X) = a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$ in $R/(f)$ the 'word' $a = (a_0, a_1, \ldots, a_{n-1}) \in {\mathbb{F}_q}^n$.

Definition 1 *(cf. [4]) Let $f \in R$ be of degree n. If $I = (f)$ is a two sided ideal of R, then an* **ideal**[1] **θ-code $\mathcal{C}$** *is a left ideal $(g)/(f) \subset R/(f)$, where $g \in R$ is a right divisor of f in R.*
If the order of θ divides n then,

1. *If $f = X^n + c$ with $c \in \mathbb{F}_q^\theta$, then we call the ideal θ-code corresponding to the left ideal $(g)/(X^n + c) \subset R/(X^n + c)$ an* **ideal θ-constacyclic code**.
2. *If $f = X^n - 1$, then we call the ideal θ-code corresponding to the left ideal $(g)/(X^n - 1) \subset R/(X^n - 1)$ an* **ideal θ-cyclic code**.

An ideal θ-cyclic code $\mathcal{C}$ has the following property ([3], Theorem 1)

$$(a_0, a_1, \ldots, a_{n-1}) \in \mathcal{C} \quad \Rightarrow \quad (\theta(a_{n-1}), \theta(a_0), \theta(a_1), \ldots, \theta(a_{n-2})) \in \mathcal{C}.$$

If θ is not the identity, then the non commutative ring R is not a unique factorisation ring and there are much more right factors of $f \in R$ than in the commutative case, leading to a huge number of linear codes that are not cyclic codes (cf. [3, 4]).

Example. Let α be a generator of the multiplicative group of $\mathbb{F}_4$ and θ the Frobenius automorphism given by $\theta(a) = a^2$. The polynomial $X^2 + \alpha^2 X + \alpha$ is a right divisor of $X^4 - 1 \in \mathbb{F}_4[X, \theta]$ so it generates a $[4, 2]_4$ ideal θ-cyclic code. Note that there are seven different monic right factors of degree two of $X^4 - 1$ in $\mathbb{F}_4[X, \theta]$ ([3], Example 2). ∎

In order to generate a two sided ideal of R, a monic polynomial f must be of the form $X^t \tilde{f}$ where $\tilde{f}$ is a monic polynomial belonging to the center $\mathbb{F}_q^\theta[X^m]$ of R, where m is the order of θ. If f is in the center of R, then we call the ideal θ-code, corresponding to the left ideal $(g)/(f) \subset R/(f)$, an *ideal θ-central code* (cf [4]).
The length of an ideal θ-code is determined by the degree of f, while the code itself is given by the generator matrix

$$G = \begin{pmatrix} g_0 & \ldots & g_{r-1} & g_r & 0 & \ldots & 0 \\ 0 & \theta(g_0) & \ldots & \theta(g_{r-1}) & \theta(g_r) & \ldots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & & & & & & \\ 0 & \ldots & 0 & \theta^{n-r-1}(g_0) & \ldots & \theta^{n-r-1}(g_{r-1}) & \theta^{n-r-1}(g_r) \end{pmatrix}$$

depending only on g.

The restriction on the length is that f has to be a multiple of the bound g^* of g, which is the generator of the smallest two sided ideal contained in the left ideal $(g) \subset R$. The degree of the bound g^* can be bounded in terms of the degree of g and the order of θ ([4], Lemma 10) namely $\deg(g^*) \leq \lambda \cdot \deg(g)$ where λ is at most $m \cdot [\mathbb{F}_q : \mathbb{F}_q^\theta]$. Over $\mathbb{F}_4$, we proved that $\lambda = 2$ when $\theta \neq id$ (lemma 11 of [4]).

[1] In previous work we called those codes simply θ-codes, but we added *ideal* in the definition in order to distinguish those codes from the module codes which we will introduce in the next section.

Any polynomial $g \in R$ of degree r always generates an ideal θ-code of length $n \geq \lambda \cdot r$. But if $n < \lambda \cdot r$, then those polynomials $g \in R$ of degree r for which $n < \deg(g^*)$ do not generate an ideal θ-code of length n. This restriction is the motivation in the following section to generalize the notion of ideal θ-codes to module θ-codes.

EXAMPLE. Consider $g = X^3 + \alpha^2 X^2 + \alpha X + 1 \in \mathbb{F}_4[X, \theta]$. Its bound $g^* = X^6 + 1$ is of degree 6. Therefore the above matrix G obtained from the coefficients of g will generate an ideal θ-code only if the length of the code is at least 6, i.e. if there are at least 3 lines in the above matrix. The use of modules instead of ideals will allow to consider also generator matrices with less lines. ∎

Note that the bound of an element $g \in \mathbb{F}_4[X, \theta]$ can also be of degree strictly less than $2 \cdot \deg(g)$:

EXAMPLE. Consider $g = X^4 + X^3 + \alpha^2 X^2 + X + \alpha \in \mathbb{F}_4[X, \theta]$. Its bound $g^* = X^6 + X^4 + X^2 + 1$ is of degree $6 < 2 \cdot 4$. Therefore from the above matrix G obtained from the coefficients of g we can generate an ideal θ-code $(g)/(X\, g^*) \subset R/(X\, g^*)$ of length 7 whose minimum distance 4 is the best known distance for $[7, 3]_4$ linear codes. ∎

1.2 Module θ-codes

The goal of this section is to define codes as modules instead of ideals.

In the following we will consider left R-modules ${}_RM$, where ${}_RM$ is an additive group with a left scalar multiplication ${}_RM \times R \to {}_RM$ given by $(m, r) \mapsto r \cdot m$. Since R is left and right Euclidean, all left ideals of R are principal of the form Rf and are examples of left R-modules as well as the quotients R/Rf. The fact that R is a left and right Euclidean ring also implies a similar structure theorem than for finitely generated abelian groups

Theorem 1 *([1], Theorem 3.3.6) A finitely generated right R-module is isomorphic to*

$$R/Rf_1 \oplus R/Rf_2 \oplus \ldots \oplus R/Rf_\ell \oplus R^r$$

where s and r are non negative integers and the f_i are non units of R with the property that f_i is a right divisor of f_{i+1} for $i \in \{1, \ldots, \ell - 1\}$.

In particular a left R-module is irreducible if and only if the module is isomorphic to R/Rf where f is irreducible in R. Note that $Rf \subset Rg$ if and only if g is a right factor of f. If $f = hg$, then Rg/Rf is a submodule of R/Rf which is cyclic and generated as a left R-module by $g + Rf$.

If $f = hg \in R$, then $Rg/Rf \cong R/Rh$. For $\ell \in R$ the module $R/R\ell$ can be identified with the set of possible remainders of a right division by ℓ in R and is therefore a $\mathbb{F}_q$-vector space of dimension $\deg(\ell)$. Therefore the left R-submodule $Rg/Rf \subset R/Rf$ is a $\mathbb{F}_q$-vector subspace of dimension $\deg(h) = \deg(f) - \deg(g)$ of the $\mathbb{F}_q$-vector space R/Rf of dimension $\deg(f)$. Since a vector subspace of a finite dimensional $\mathbb{F}_q$-vector space is a code over $\mathbb{F}_q$, we obtain the following generalization of ideal θ-codes (cf. [4]) :

Definition 2 *Let $f \in R$ be of degree n. A* module θ-code $\mathcal{C}$ *is a left R-submodule $Rg/Rf \subset R/Rf$ where g is a right divisor of f in R. Its length is $n = \deg(f)$, its dimension is $k = \deg(f) - \deg(g)$ and if its distance is d then we say that the code $\mathcal{C}$ is of type $[n, k, d]_q$.*

As usual, we identify codewords with the list of coefficients of the remainder of a right division by f in R. The elements of Rg/Rf are then all left multiples of $g = g_r X^r + \cdots + g_1 X + g_0$ and are of the form

$$\left(\sum_{i=0}^{\deg(f)-\deg(g)-1} b_i X^i \right) \cdot g$$

This shows that the generator matrix of the corresponding module θ-code of length $n = \deg(f)$ is given by the matrix G in the previous section.

Note that the code is defined uniquely by the generator polynomial g whose leading coefficient can be supposed to be one. Therefore a module θ-code of type $[n, k] = [n, n - \deg(g)]$ is defined by the $\deg(g) - 1$ coefficients of the monic polynomial g, and there are $(\deg(g) - 1)^q$ such codes.

Since the restriction linked to the degree of the bound g^* of g no longer exists, there are more module θ-codes than ideal θ-codes. In particular any polynomial $g \in R$ is a right divisor of some polynomial f of degree $n \geq \deg(g)$, so for any $g \in R$ and any $n \geq \deg(g)$ the matrix G generates a module θ-code.

Example. The previous polynomial $g = X^3 + \alpha^2 X^2 + \alpha X + 1 \in \mathbb{F}_4[X, \theta]$ with bound $g^* = X^6 + 1$ generates, via the matrix

$$G = \begin{pmatrix} 1 & \alpha & \alpha^2 & 1 & 0 \\ 0 & 1 & \alpha^2 & \alpha & 1 \end{pmatrix}$$

a $[5, 2]_4$ module θ-code over $\mathbb{F}_4$ which is not an ideal θ-code and whose minimum distance 4 matches the best known distance for $[5, 2]_4$ linear codes. ∎

2 Examples of distance improvements by using modules instead of ideals

The following table illustrates the gain of using module θ-codes instead of just ideal θ-codes.

In the table, n is the length of the module θ-codes over $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ and corresponds to the degree of f . The integer r is the degree of g (therefore $n - r$ is the dimension of the code). An entry C_d indicates that the best known linear $[n, n - r]_4$ code is of minimal distance d and can be found within the family of cyclic codes. An entry C_d^θ indicates that the best known linear $[n, n - r]_4$ code is of minimal distance d and can be found within the family of ideal θ-cyclic codes (the entry C_{ds}^θ indicates that there exists such a code which is Euclidean self dual). An entry θ_d indicates that the best known linear $[n, n - r]_4$ code is of minimal distance d and can be found within the family of ideal θ-codes. An

$n \setminus r$	2	3	4	5	6	7	8	9	10	11
3	$\mathbf{M_3}$									
4	C_{3s}^{θ}	C_4								
5	-1	$\mathbf{M_4}$	$\mathbf{M_5}$							
6	C_2	C_4	C_4^{θ}	C_6						
7	θ_2	θ_3	θ_4	$\mathbf{M_5}$	$\mathbf{M_7}$					
8	C_2	C_3^{θ}	C_{4s}^{θ}	C_5^{θ}	C_6^{θ}	C_8				
9	θ_2	θ_3	θ_4	$\mathbf{M_5}$	$\mathbf{M_6}$	$\mathbf{M_7}$	$\mathbf{M_9}$			
10	C_2	θ_3	C_4^{θ}	C_5^{θ}	C_6^{θ}	θ_6	θ_8	C_{10}		
11	θ_2	θ_3	θ_4	θ_4	$\mathbf{M_6}$	$\mathbf{M_6}$	$\mathbf{M_7}$	$\mathbf{M_8}$	$\mathbf{M_{11}}$	
12	C_2	θ_3	θ_4	C_4	C_{6s}^{θ}	C_6^{θ}	C_7^{θ}	C_8^{θ}	C_9^{θ}	C_{12}
13	θ_2	θ_3	θ_4	θ_4	θ_5	$\mathbf{M_6}$	$\mathbf{M_7}$	$\mathbf{M_8}$	$\mathbf{M_9}$	$\mathbf{M_{10}}$
14	C_2	C_3^{θ}	C_4^{θ}	C_4	C_5^{θ}	C_{6s}^{θ}	C_7^{θ}	$\mathbf{M_8}$	$\mathbf{M_9}$	C_{10}^{θ}
15	θ_2	-1	-1	θ_4	θ_5	-1	-1	$\mathbf{M_8}$	$\mathbf{M_8}$	-1
16	C_2	-1	-1	C_4^{θ}	-1	-1	-1	-1	C_8^{θ}	$\mathbf{M_9}$
17	θ_2	-1	-1	θ_4	-1	-1	-1	-1	$\mathbf{M_8}$	$\mathbf{M_9}$
18	C_2	-1	θ_3	θ_4	-1	-1	C_6^{θ}	-1	C_8^{θ}	-1
19	θ_2	-1	θ_3	θ_4	-1	-1	θ_6	θ_7	$\mathbf{M_8}$	θ_8
20	C_2	-1	θ_3	θ_4	-1	-1	θ_6	C_7^{θ}	C_8^{θ}	C_8^{θ}
21	θ_2	-1	θ_3	θ_4	-1	θ_5	-1	-1	θ_7	θ_8
22	C_2	θ_2	θ_3	θ_4	θ_4	θ_5	-1	C_6^{θ}	C_7^{θ}	C_8

Table 1: Codes over $\mathbb{F}_4$ constructed using $R = \mathbb{F}_4[X, \theta]$, where $\mathrm{id} \neq \theta \in \mathrm{Aut}(\mathbb{F}_4)$.

entry M_d indicates that the best known linear $[n, n-r]_4$ code is of minimal distance d and can be found within the family of module θ-codes. A negative entry $-j$ indicates that the best module θ-code has a distance $d - j$, where d is the distance of the best known linear $[n, n-r]_4$ code.

In the part of the table below the diagonal staircase, there is no restriction on the generators of an ideal θ-code due to the bound. Therefore module θ-codes will not improve ideal θ-codes in this lower part of the table.

Example. The polynomial $g = X^9 + \alpha X^8 + X^7 + X^5 + \alpha^2 X^4 + \alpha X^2 + X + 1$ generates a module θ-code of any length ≥ 9. As its bound is $X^{18} + X^{16} + X^{14} + X^{12} + X^{10} + X^6 + 1$, the module θ-code of length 14 generated by g is not an ideal θ-code. Its minimum distance is 8, which is the best known distance for $[14, 5]_4$ linear codes. Furthermore there is no $[14, 5]_4$ ideal θ-code reaching this best distance. In the table this code corresponds to the entry M_8 at line 14 and column $9 = 14 - 5$. ∎

In [3, 5] the BCH approach is generalized to the non-commutative case to construct codes of arbitrary length and prescribed distance. In the following, we show that this approach can be extended to the module θ-codes. The difference with the work in [3, 5] is

that the use of module θ-codes allows to remove the restriction on the length of the codes in terms of the bound of g ([4], Definition 9). We get the following definition derived from definition 5 of [5]:

Definition 3 *Let $\theta \in Aut(\mathbb{F}_q)$ be given by $a \mapsto a^{q_0}$, δ be a positive integer, $q = q_0^t$ and β belong to a field extension $\mathbb{F}_{q_0^s}$ of $\mathbb{F}_q = \mathbb{F}_{q_0^t}$. A* BCH module θ-code over $\mathbb{F}_q$ with parameters δ and β of length n *is a module θ-code of length n generated by the monic skew polynomial $g \in \mathbb{F}_q[X, \theta]$ of smallest degree such that g is right divisible in $\mathbb{F}_{q_0^s}[X, \theta]$ by $X - \beta^i$ for $i \in \{0, \ldots, \delta - 1\}$.*

For the construction of the generator polynomial g of a BCH module θ-code we can use the algorithm given in [5] Section 4. The decoding algorithm described in [3, 5] also allows to decode skew BCH module codes. The proof of Proposition 2 of [5] can be adapted word for word in order to obtain

Proposition 1 *Let $\mathcal{C}$ be a BCH module θ-code with the notations of the above definition. If $n \leq (q_0 - 1) \cdot s$ and β is of order $q_0^s - 1$ then $\mathcal{C}$ has minimum distance at least δ.*

The following proposition improves the previous one for codes defined over $\mathbb{F}_q = \mathbb{F}_{2^t}$, showing that β does not need to be a generator of the field extension $\mathbb{F}_{2^s}$:

Proposition 2 *Let $\mathcal{C}$ be a BCH module θ-code with the notations of definition (cf. 3) and $q_0 = 2$. If the order of β is at least $2^n - 1$ then $\mathcal{C}$ has a minimum distance at least δ.*

Proof. Let m be the order of β. Following the proof of proposition 2 of [5] or the proposition 2 of [3], the minimum distance of $\mathcal{C}$ is at least δ if and only if for all $j < i < n$, $\beta^{(2^i - 2^j)/(2-1)} \neq 1$. Let us assume $\beta^{2^i - 2^j} = 1$, then the order m of β divides $2^i - 2^j$; as m divides $2^s - 1$, it cannot divide 2^j, so there exists $l < n$ such that m divides $2^l - 1$. As $l < n$ we get $m < 2^n - 1$. So if $m \geq 2^n - 1$ then the minimum distance of $\mathcal{C}$ is at least δ. ∎

Using module θ-codes allows to remove the restriction on the length of the code due to the bound of g and therefore allows to find more such skew BCH codes when the degree of g is large compared to the length of the code (i.e. k is small). The following examples show that there are more BCH module θ-codes than BCH ideal θ-codes.

Example. Using modules we construct a $[10, 4, 6]_4$ BCH module θ-code (best possible distance). This code is obtained using the element $\beta = a^{11} \in \mathbb{F}_{2^{12}}$ of order $2^{12} - 1$ (where a is a generator of the multiplicative group of $\mathbb{F}_{2^{12}}$ used by Magma) by imposing a distance 2. The resulting generator polynomial is $g = X^6 + \alpha^2 X^5 + \alpha X^4 + \alpha X^2 + X + \alpha^2$ (where $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$). The bound of g is $g^* = X^{12} + 1$, showing that the smallest length of an ideal θ-code with generator polynomial g is 12. This code improves the BCH ideal θ-codes as there exists no $[10, 4]$ BCH ideal θ-code constructed from $\mathbb{F}_{2^{12}}$ ([5]). ∎

Example. Using modules we construct the module θ-codes $[8, 3, 5]_4$ and $[8, 2, 6]_4$ respectively (best possible distances) obtained from $\mathbb{F}_{2^{12}} = \mathbb{F}_2(a)$ (where a is a generator of the multiplicative group of $\mathbb{F}_{2^{12}}$ used by Magma) by imposing a distance 2. No code with such length and dimension can be constructed using ideal θ-codes ([5])

1. In order to construct a $[8,3,5]_4$ module θ-code we used $\beta = a^{25} \in \mathbb{F}_{2^{12}}$ of order $819 \neq 2^{12}-1$, $819 \geq 2^8-1$ to obtain $g = X^5 + \alpha^2 X^4 + \alpha^2 X^2 + \alpha X + \alpha^2 \in \mathbb{F}_4[X,\theta]$ whose bound is $g^* = X^{10} + X^8 + X^6 + X^4 + X^2 + 1$

2. In order to construct a $[8,2,6]_4$ module θ-code, we used $\beta = a \in \mathbb{F}_{2^{12}}$ to obtain $g = X^6 + X^5 + \alpha^2 X^4 + X^3 + \alpha X^2 + \alpha^2 X + \alpha^2 \in \mathbb{F}_4[X,\theta]$ whose bound is $g^* = X^{12} + 1$.

■

3 Self-dual module θ-codes

The Euclidean and Hermitian dual of an ideal θ-cyclic code $(g)/(X^n-1)$ is an ideal θ-cyclic code whose generator polynomial depends on the factor h in the decomposition $X^n - 1 = hg = gh$ (cf. [4]). This allowed us in [4] to characterise self-dual codes by polynomial equations satisfied by the coefficients of g. However, if an ideal θ-code is not θ-cyclic then its dual may not be an ideal θ-code and until now we were not able to characterize those ideal θ-central codes whose duals are ideal θ-central codes.

In the following we give a characterization of the module θ-codes whose duals are module θ-codes. Like in [4] we derive polynomial equations which characterize self-dual module θ-codes. Thanks to a refinement in the resolution of these polynomial equations we were able to find two new $[56,28,15]_4$ non equivalent Euclidean self-dual codes, improving the previous $[56,28,14]_4$ self-dual codes. It turns out that these two module θ-codes are ideal θ-cyclic codes.

3.1 Dual for the Euclidean scalar product

The Euclidean dual $\mathcal{C}^\perp$ of a code $\mathcal{C}$ of ${\mathbb{F}_q}^n$ is the set of words which are orthogonal to the code's words relatively to the Euclidean scalar product. We characterize those module θ-codes whose duals are module θ-codes, extending the corresponding result of [4] for ideal θ-cyclic codes.

In the following we will assume that the constant term of the generator polynomial g is $\neq 0$. This is not a strong restriction since if g is right divisible by X^s, then the resulting ideal θ-code has s coordinates which are always zeros and the resulting code is of little interest if $s > 0$ (cf. [4], Proposition 13).

Proposition 3 (Euclidean dual of a module θ-code) *Let $k \leq n$ be integers, $g \in \mathbb{F}_q[X,\theta]$ of degree $n-k$ with constant term $\neq 0$ and $\mathcal{C}$ be the module θ-code of length n generated by g.*
The Euclidean dual $\mathcal{C}^\perp$ of $\mathcal{C}$ is a module θ-code generated by a polynomial of degree k with constant term $\neq 0$ if and only if there exists $h \in \mathbb{F}_q[X,\theta]$ and c in $\mathbb{F}_q - \{0\}$ such that $g\,h = X^n - c$ (i.e. the remainder of the left division of $X^n \in \mathbb{F}_q[X,\theta]$ by g is a non zero

constant).
In this case the generator polynomial of $\mathcal{C}^{\perp}$ *is given by :*

$$g^{\perp} = \sum_{i=0}^{k} \theta^i(h_{k-i})\, X^i$$

and $g^{\perp}$ *is a left divisor of* $X^n - \theta^{k-n}\left(\frac{1}{c}\right) \in \mathbb{F}_q[X,\theta]$.

PROOF.

- Suppose that $X^n - gh = c \neq 0$ in $\mathbb{F}_q[X,\theta]$ and define $g^{\perp} := \sum_{i=0}^{k} \theta^i(h_{k-i})\, X^i$. As $g_0 h_0 = c \neq 0$ and $g_0 \neq 0$, we must have $h_0 \neq 0$. Therefore $g^{\perp}$ is a polynomial of degree k and generates a module θ-code $\tilde{\mathcal{C}}$ of length n and dimension $n-k$. We now prove that $\tilde{\mathcal{C}} = \mathcal{C}^{\perp}$ by showing that the words of $\mathcal{C}$ and $\tilde{\mathcal{C}}$ are orthogonal:
  For $i_0 \in \{0,\ldots,k-1\}, i_1 \in \{0,\ldots,n-k-1\}$ we have $< X^{i_0} g, X^{i_1} g^{\perp} >$

$$\begin{aligned}
&= < \sum_{i=0}^{n-k} \theta^{i_0}(g_i)\, X^{i+i_0}, \sum_{i=0}^{k} \theta^{i_1}(\theta^i(h_{k-i}))X^{i+i_1} > \\
&= < \sum_{i=0}^{n-k} \theta^{i_0}(g_i)\, X^{i+i_0}, \sum_{i=i_1-i_0}^{i_1-i_0+k} \theta^{i+i_0}(h_{k-i+i_1-i_0})X^{i+i_0} > \\
&= \sum_{i=\max(0,i_1-i_0)}^{\min(n-k,i_1-i_0+k)} \theta^{i_0}(g_i)\theta^{i+i_0}(h_{k-i+i_1-i_0}) \\
&= \theta^{i_0}\left(\sum_{i=\max(0,l-k)}^{\min(n-k,l)} g_i \theta^i(h_{l-i})\right) \qquad (\text{where } l = k+i_1-i_0 \in \{1,\ldots,n-1\}) \\
&= \theta^{i_0}\left((gh)_l\right) \qquad (\text{here } (gh)_l \text{ denotes the coefficient of } X^l \text{ in } gh) \\
&= 0 \qquad (\text{because } gh = X^n - c)
\end{aligned}$$

- Conversely, suppose that $\mathcal{C}^{\perp}$ is a module θ-code generated by a polynomial $\tilde{g}$ with constant term $\neq 0$. Define h as $h = \sum_{i=0}^{k} \theta^{i-k}(\tilde{g}_{k-i})X^i \in \mathbb{F}_q[X,\theta]$. Since the constant term of $\tilde{g}$ is $\neq 0$, the polynomial h is of degree k. Then for all $i_0 \in \{0,\ldots,k\}$, $i_1 \in \{0,\ldots,n-k\}$,

$$\begin{aligned}
0 &= < X^{i_0} g, X^{i_1} \tilde{g} > \\
&= < \sum_{i=0}^{n-k} \theta^{i_0}(g_i)\, X^{i+i_0}, \sum_{i=0}^{k} \theta^{i_1}(\tilde{g}_i)X^{i+i_1} > \\
&= < \sum_{i=0}^{n-k} \theta^{i_0}(g_i)\, X^{i+i_0}, \sum_{i=i_1-i_0}^{k+i_1-i_0} \theta^{i_1}(\tilde{g}_{i-i_1+i_0})X^{i+i_0} > \\
&= \sum_{i=max(0,i_1-i_0)}^{min(n-k,i_1-i_0+k)} \theta^{i_0}(g_i)\theta^{i_1}(\tilde{g}_{i-i_1+i_0})
\end{aligned}$$

So for all $l \in \{1, \ldots, n-1\}$ $(l = i_1 - i_0 + k)$

$$\begin{aligned} 0 &= \theta^{i_0}\left(\sum_{i=max(0,l-k)}^{min(n-k,l)} g_i \theta^{l-k}(\tilde{g}_{i+k-l})\right) \\ &= \theta^{i_0}\left(\sum_{i=max(0,l-k)}^{min(n-k,l)} g_i \theta^{i}(h_{l-i})\right) \\ 0 &= \sum_{i=max(0,l-k)}^{min(n-k,l)} g_i \theta^{i}(h_{l-i}) \qquad \text{(the coefficient of } X^l \text{ in } gh) \end{aligned}$$

This shows that gh is of the form $X^n + c$ with $c \in \mathbb{F}_q$. Since $g_0 h_0 = g_0 \theta^{-k}(\tilde{g}_k) \neq 0$ we have that $c \neq 0$.

- Denote $\mathbb{F}_q(X, \theta)$ the right field of fraction of $\mathbb{F}_q[X, \theta]$ and X^{-1} the inverse of X. We have $aX^{-1} = X^{-1}\theta(a)$ and $\sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} X^{-i} a_i$ is an anti-morphism of $\mathbb{F}_q(X, \theta)$ (cf. proof of Lemma 17 in [4]). If $gh = X^n - c$ then

$$X^k \varphi(h)\varphi(g) X^{n-k} = X^k (1/X^n - c) X^{n-k} = 1 - \theta^k(c) X^n \in \mathbb{F}_q[X, \theta].$$

As $g^{\perp} = X^k \varphi(h)$, we obtain that $g^{\perp}$ is a left divisor of $1 - \theta^k(c) X^n \in \mathbb{F}_q[X, \theta]$ so it is a left divisor of $-(1 - \theta^k(c) X^n)\theta^{-n+k}(\frac{1}{c}) = X^n - \theta^{k-n}(\frac{1}{c})$.

∎

When a module θ-code is generated by a polynomial satisfying the conditions of the proposition, one can deduce a nice expression for the parity check matrix of the code.

Corollary 1 (Parity check matrix) *Let $k \leq n$ be integers, let $g \in \mathbb{F}_q[X, \theta]$ be of degree $n - k$ with constant term $\neq 0$. If there exists $c \in \mathbb{F}_q - \{0\}$ and $h \in \mathbb{F}_q[X, \theta]$ such that $gh = X^n - c$, then the parity check matrix of the module θ-code $\mathcal{C}$ of length n generated by g is:*

$$H = \begin{pmatrix} h_k & \ldots & \theta^{k-1}(h_1) & \theta^k(h_0) & 0 & \ldots & 0 \\ 0 & \theta(h_k) & \ldots & \ldots & \theta^{k+1}(h_0) & \ldots & 0 \\ 0 & \ddots & \ddots & & & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ldots & \ddots & 0 \\ 0 & \ldots & 0 & \theta^{n-k-1}(h_k) & \ldots & \theta^{n-2}(h_1) & \theta^{n-1}(h_0) \end{pmatrix}$$

Proof. The parity check matrix of $\mathcal{C}$ is the matrix of the dual $\mathcal{C}^{\perp}$. As g satisfies the conditions of proposition 3, $\mathcal{C}^{\perp}$ is a module θ-code with generator polynomial $h_k + \cdots + \theta^{k-1}(h_1)\, X^{k-1} + \theta^k(h_0)\, X^k$. ∎

Example.

1. Consider the polynomial $g = X^2 + \alpha X + 1 \in \mathbb{F}_4[X, \theta]$, where $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$. Since $X^3 - g(X + \alpha) = \alpha \neq 0$, the proposition shows that the dual of the $[3, 1]_4$ module θ-code $\mathcal{C}$ generated by g is a module θ-code generated by $g^\perp = 1 + \alpha^2 X$. The parity check matrix of $\mathcal{C}$ is:
$$H = \begin{pmatrix} 1 & \alpha^2 & 0 \\ 0 & 1 & \alpha \end{pmatrix}$$

2. Consider the polynomial $g = X^4 + \alpha^3 \in \mathbb{F}_8[X, \theta]$, where $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ and $\alpha^3 + \alpha + 1 = 0$ and θ is the Frobenius automorphism. The polynomial $g = X^4 + \alpha^3$ generates a $[8, 4]_8$ module θ-code $\mathcal{C}$. Since $X^8 - g(X^4 + \alpha^5) = \alpha \neq 0$, the dual of the code $\mathcal{C}$ is a module θ-code generated by : $1 + \theta^4(\alpha^5)X^4 = 1 + \alpha^3 X^4$ and the parity check matrix of $\mathcal{C}$ is deduced from it.

■

In [4], we prove that the dual of an ideal θ-cyclic code is θ-cyclic. This result can be seen as a consequence of the previous proposition :

Corollary 2 (Euclidean dual of an ideal θ-cyclic code) *The dual code of an ideal θ-constacyclic code is an ideal θ-constacyclic code.*

PROOF. The generator polynomial g of an ideal θ-constacyclic code of length n is a right divisor of $X^n - c \in R = \mathbb{F}_q[X, \theta]$, where $c \in \mathbb{F}_q^\theta$ and n is a multiple of the order of θ. Since $X^n - c$ belongs to the center of R, the polynomial g is also a left divisor of $X^n - c \in R$. According to proposition 3, the code $\mathcal{C}^\perp$ is a module θ-code whose generator polynomial $g^\perp$ is a left divisor of $X^n - \theta^{k-n}(\frac{1}{c}) = X^n - \frac{1}{c}$. Since $X^n - 1/c$ belongs to the center of R, we have that $g^\perp$ is also a right divisor of $X^n - 1/c$. The central polynomial $X^n - \frac{1}{c}$ generates a two-sided ideal of R, showing that $\mathcal{C}^\perp$ is an ideal θ-constacyclic code. ■

The dual of an ideal θ-central code is not always an ideal θ-central code (examples 5 and 20 of [4]). The above proposition allows to characterize the ideal θ-central codes whose duals are again θ-central codes.

Corollary 3 (Euclidean dual of an ideal θ-central code) *Let $k \leq n$ be integers, let $\mathcal{C}$ be an ideal θ-central code of length n generated by a polynomial g of degree $n - k$ and constant term $\neq 0$. The code $\mathcal{C}^\perp$ is an ideal θ-central code if and only if*

1. *there exists $h \in \mathbb{F}_q[X, \theta]$ and a non zero constant c such that $X^n - c = gh$ (i.e. the remainder of the left division of X^n by g is a non zero constant);*
2. *the degree of the bound $(g^\perp)^*$ of $g^\perp = \sum_{i=0}^{k} \theta^i(h_{k-i})\, X^i$ is $\leq n$.*

In this case the ideal θ-central code $\mathcal{C}^\perp$ is generated by $g^\perp$.

PROOF. A module θ-code with generator g and length n is a central θ-code if and only if the degree of the bound of g is $\leq n$. The result now follows from proposition 3. ■

EXAMPLE.

1. The polynomial $g = X^3 + X^2 + X + \alpha \in \mathbb{F}_4[X, \theta]$ generates an ideal θ-central code (which is not θ-cyclic) of length 12 (examples 5 and 20 in [4]). Since the remainder $X^2 + \alpha^2 X + \alpha$ of the left division of X^{12} by g is not a constant, the code $\mathcal{C}^\perp$ is not a module θ-code and therefore also not an ideal θ-central code.

2. The polynomial $g = X^2 + \alpha \in \mathbb{F}_4[X, \theta]$ generates a module θ-code $\mathcal{C}$ of length 4. The bound of g is $g^* = X^4 + X^2 + 1$, showing that this code is an ideal θ-central code which is not θ-cyclic. Since the remainder α^2 of the left (and right in this case) division of X^4 by g is a non zero constant, the above proposition shows that the dual code is a module θ-code generated by $g^\perp = X^2 + \alpha^2$. As the bound of $g^\perp$ is $X^4 + X^2 + 1$ is of degree ≤ 4, the code $\mathcal{C}^\perp$ is an ideal θ-central code.

3. The polynomial $g = X^2 + \alpha \in \mathbb{F}_4[X, \theta]$ also generates an ideal θ-central code of length 8 which is not θ-cyclic. Since the remainder α of the left (and right in this case) division of X^8 by g is a non zero constant, the above proposition shows that the dual code is a module θ-code generated by $g^\perp = X^6 + \alpha^2 X^4 + \alpha X^2 + 1$. As the bound of $g^\perp = X^{12} + X^{10} + X^6 + X^2 + 1$ is of degree > 8, the code $\mathcal{C}^\perp$ is a module θ-code which is not an ideal θ-central code.

■

A code is said to be self-dual if it is equal to its dual. Following [4], we characterize Euclidean self-dual module θ-codes with a system of polynomial equations.

Corollary 4 (Euclidean self-dual module θ-codes) *Let k be an integer and the polynomial $g = \sum_{i=0}^{k} g_i X^i \in \mathbb{F}_q[X, \theta]$ be monic of degree k and constant term $g_0 \neq 0$. Denote $\mathcal{C}$ the module θ-code of length $2k$ generated by g. The code $\mathcal{C}$ is Euclidean self-dual if, and only if,*

$$\forall l \in \{1, \ldots, k\}, \sum_{i=0}^{l} \theta^{k-l}(g_i)\, g_{i+k-l} = 0 \tag{1}$$

Proof. The module θ-code $\mathcal{C}$ is self-dual if, and only if, $\mathcal{C}^\perp$ is a module θ-code whose (monic) generator polynomial $g^\perp$ is equal to g. According to proposition (3), $\mathcal{C}^\perp$ is a module θ-code if and only if there exists $c \in \mathbb{F}_q - \{0\}$ and $h \in \mathbb{F}_q[X, \theta]$ such that $gh = X^{2k} - c$ and its (monic) generator polynomial is $g^\perp = \sum_{i=0}^{k} \theta^i(h_{k-i})/\theta^k(h_0)\, X^i$. So the code $\mathcal{C}$ is self-dual if, and only if, there exists h and c such that $gh = X^{2k} - c$ where $\forall i \in \{0, \ldots, k\}$, $\theta^i(h_{k-i})/\theta^k(h_0) = g_i$ i.e. $h_i = \theta^i(c/g_0)\, \theta^{i-k}(g_{k-i})$. This is equivalent to :

$$\exists c \in \mathbb{F}_q - \{0\}, \left(\sum_{i=0}^{k} g_i X^i\right) \left(\sum_{i=0}^{k} \theta^i \left(\frac{c}{g_0}\right) \theta^{i-k}(g_{k-i}) X^i\right) = X^{2k} - c$$

$$\Leftrightarrow \quad \forall l \in \{1,\dots,2k-1\}, \quad \sum_{i=\max(0,l-k)}^{\min(k,l)} g_i \theta^i \left(\theta^{l-i} \left(\frac{c}{g_0} \right) \theta^{l-i-k}(g_{k-l+i}) \right) = 0$$
$$\Leftrightarrow \quad \forall l \in \{1,\dots,2k-1\}, \quad \sum_{i=\max(0,l-k)}^{\min(k,l)} g_i \theta^l \left(\frac{c}{g_0} \right) \theta^{l-k}(g_{k-l+i}) = 0$$

$$\Leftrightarrow \quad \forall l \in \{1,\dots,2k-1\}, \quad \sum_{i=\max(0,l-k)}^{\min(k,l)} \theta^k(g_i)\, \theta^l(g_{i-(l-k)}) = 0$$

To conclude, it suffices to notice a symetry in this system of equation, which enables to consider only the k first equations. ∎

EXAMPLE. Over $\mathbb{F}_4$ the (Euclidean) self-dual module θ-codes of length 4 are generated by the polynomials $X^2 + g_1 X + g_0$ where g_0 and g_1 satisfy the equations

$$\begin{cases} \theta(g_0)g_1 + \theta(g_1) = 0 \\ g_0^2 + g_1^2 + 1 = 0 \end{cases}$$

i.e. $g_1(g_0^2 + g_1) = 0$ and $g_0^2 + g_1^2 = 1$. We get three polynomials $X^2 + 1$, $X^2 + \alpha^2 X + \alpha$ and $X^2 + \alpha\, X + \alpha^2$. The codes they generate are self-dual and θ-cyclic. ∎

Thanks to a further simplification of the system (1) that we do not detail here, we could perform the computation of Euclidean self-dual codes over $\mathbb{F}_4$ of length ≤ 58. We found two non equivalent Euclidean self-dual $[56, 28, 15]_4$ codes which improve the best known distance (14, [6]) for self-dual codes of this length over $\mathbb{F}_4$. Here are the generator polynomials of these codes :

$$X^{28} + X^{26} + \alpha\, X^{24} + \alpha^2\, X^{22} + \alpha\, X^{21} + X^{20} + X^{19} + \alpha^2\, X^{18} + \alpha\, X^{17} + \alpha^2\, X^{16} + \alpha\, X^{15} + X^{13} + \alpha^2\, X^{12} + X^{11} + \alpha^2\, X^{10} + \alpha\, X^9 + \alpha\, X^8 + X^7 + \alpha^2\, X^6 + X^4 + \alpha\, X^2 + \alpha\ ,$$

$$X^{28} + X^{26} + \alpha\, X^{25} + \alpha^2\, X^{24} + \alpha^2\, X^{23} + X^{22} + X^{21} + \alpha\, X^{19} + \alpha\, X^{18} + \alpha^2\, X^{17} + \alpha^2\, X^{16} + \alpha^2\, X^{15} + \alpha\, X^{14} + X^{13} + X^{12} + X^{11} + \alpha\, X^{10} + \alpha\, X^9 + \alpha^2\, X^7 + \alpha^2\, X^6 + X^5 + X^4 + \alpha\, X^3 + \alpha^2\, X^2 + \alpha^2$$

It turns out that these two codes are θ-cyclic and that we found no self-dual module θ-code which is not θ-constacyclic . We conjecture that such codes do not exist, which can be proven over $\mathbb{F}_q[X, \theta]$ when $\theta \neq id$ has order 2 :

Proposition 4 *Let θ be an automorphism of order 2 of $\mathbb{F}_q$. If $\mathcal{C}$ is an Euclidean self-dual module θ-code over $\mathbb{F}_q$ generated by a polynomial with constant term $\neq 0$, then $\mathcal{C}$ is an ideal θ-constacyclic code.*

PROOF. Let the polynomial g of degree k be the generator of the Euclidean self-dual module θ-code $\mathcal{C}$. According to proposition 3, there exists a constant $c \neq 0$ and a polynomial $h \in R$ such that $gh = X^{2k} - c$. Since X^{2k} belongs to the center of R we obtain from $(gh)g = X^{2k}g - cg$ that $g(X^{2k} - hg) = cg$. We deduce that g is a left divisor of cg, showing that $cg = g\tilde{c}$ for some $\tilde{c} \in \mathbb{F}_q$. Since the constant term of g is $\neq 0$, comparing the constant terms on both sides shows that $c = \tilde{c}$ and we obtain $cg = gc$. Therefore $\forall i \in \{0,\dots,k-1\}$ we have $c\, g_i = g_i \theta^i(c)$.

Let us assume that $\theta(c) \neq c$. Then $g_i = 0$ for all odd i, which implies that k is even. From proposition 3 we obtain that the polynomial $g^\perp$ is a left divisor of $X^{2k} - \theta^{k-2k}(\frac{1}{c}) = X^{2k} - \frac{1}{c}$ (note that k is even and θ is of order 2). Since $\mathcal{C}$ is Euclidean self-dual, the polynomial $g^\perp$ is equal to $\theta^k(h_0) \cdot g$. As $X^{2k} - \frac{1}{c}$ commutes with $\theta^k(h_0)$ we get that g is a left divisor of $X^{2k} - \frac{1}{c}$. Since g is also a left divisor of $X^{2k} - c$, the polynomial g is also a left divisor of the difference of the two polynomials

$$\left(X^{2k} - \frac{1}{c}\right) - \left(X^{2k} - c\right) \;=\; c - \frac{1}{c}$$

which must therefore be zero. From $c^2 = 1$ we obtain $c = 1$ or -1, showing that $c \in \mathbb{F}_q^\theta$ and contradicting our assumption that $\theta(c) \neq c$.
Therefore g is a left and right divisor of the central polynomial $X^{2k} - c$ with $\theta(c) = c$, , which implies that $\mathcal{C}$ is an ideal θ-constacyclic code. ∎

Example. Over $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$ with $\alpha^2 - \alpha - 1 = 0$ and $\theta : a \mapsto a^3$ the (Euclidean) self-dual module θ-codes of length 12 are generated by the polynomials $X^6 + g_5X^5 + \cdots + g_1X + g_0$ where $g_0, \ldots, g_5$ satisfy the equations

$$\begin{cases} g_0^3\, g_5 + g_1^3 = 0 \\ g_0\, g_4 + g_1\, g_5 + g_2 = 0 \\ g_0^3\, g_3 + g_1^3\, g_4 + g_2^3\, g_5 + g_3^3 = 0 \\ g_0\, g_2 + g_1\, g_3 + g_2\, g_4 + g_3\, g_5 + g_4 = 0 \\ g_0^3\, g_1 + g_1^3\, g_2 + g_2^3\, g_3 + g_3^3\, g_4 + g_4^3\, g_5 + g_5^3 = 0 \\ g_0^2 + g_1^2 + g_2^2 + g_3^2 + g_4^2 + g_5^2 + 1 = 0 \end{cases}$$

Solving the corresponding polynomial system, we find 40 solutions in $\mathbb{F}_9^6$; one of these gives the polynomial $X^6 + 2X^5 + \alpha^3X^4 + \alpha^2X^3 + \alpha X^2 + X + 1$ which divides on the right the polynomial $X^{12} + 1$. It generates an Euclidean self-dual $[12, 6, 6]_9$ ideal θ-constacyclic code.
∎

For the Hermitian scalar product, we find self-dual module θ-codes which are not θ-constacyclic.

3.2 Dual for the Hermitian scalar product

Let q be an even power of a prime number and let θ be the automorphism of order 2 over $\mathbb{F}_q$: $a \mapsto a^{\sqrt{q}}$. The *Hermitian scalar product* is defined over ${\mathbb{F}_q}^n$ by

$$\forall x, y \in {\mathbb{F}_q}^n,\ < x, y >_H = \sum_{i=1}^{n} x_i \cdot \theta(y_i)$$

i.e.

$$< x, y >_H = < x, \theta(y) >$$

The Hermitian dual of a code of ${\mathbb{F}_q}^n$ is the set of words which are orthogonal to the code's words relatively to the Hermitian scalar product.

Proposition 5 (Hermitian dual of a module θ-code) *Let $k \leq n$ be integers, $g \in \mathbb{F}_q[X,\theta]$ of degree $n-k$ with constant term $\neq 0$ and $\mathcal{C}$ be the module θ-code of length n generated by g.*
The Hermitian dual $\mathcal{C}^H$ of $\mathcal{C}$ is a module θ-code generated by a polynomial of degree k with constant term $\neq 0$ if and only if there exists $h \in \mathbb{F}_q[X,\theta]$ and c in $\mathbb{F}_q - \{0\}$ such that $g\,h = X^n - c$ (i.e. the remainder of the left division of $X^n \in \mathbb{F}_q[X,\theta]$ by g is a non zero constant).
In this case the generator polynomial of $\mathcal{C}^H$ is given by :

$$g^H = \sum_{i=0}^{k} \theta^{i+1}(h_{k-i})\, X^i = \phi(g^{\perp})$$

where $\phi(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} \theta(a_i) X^i$. Lastly, g^H divides the polynomial $X^n - \theta^{k-n+1}(1/c)$ on the left.

Proof. The proof is based on the proposition 3 and the equality

$$\forall i_0 \in \{0,\ldots,k\}, \forall i_1 \in \{0,\ldots,n-k\}, < X^{i_0} g, X^{i_1} g^H >_H = < X^{i_0} g, X^{i_1} \phi(g^H) > = < X^{i_0} g, X^{i_1} g^{\perp} >$$

■

Corollary 5 (Hermitian self-dual module θ-codes) *Let $k \in \mathbb{N}$ and $g \in \mathbb{F}_q[X,\theta]$ be a monic polynomial of degree k and constant term $\neq 0$. Let $\mathcal{C}$ be the module θ-code of length $2k$ generated by g. The code $\mathcal{C}$ is Hermitian self-dual if, and only if,*

$$\forall l \in \{1,\ldots,k\}, \sum_{i=0}^{l} \theta^{k-l-1}(g_i)\, g_{i+k-l} = 0 \tag{2}$$

Proof. We use the same techniques as in the lemma for Euclidean self-dual codes. ■

Example. Over $\mathbb{F}_4$ the (Hermitian) self-dual module θ-codes of length 4 are generated by the polynomials $X^2 + g_1 X + g_0$ where g_0 and g_1 satisfy the equations

$$\begin{cases} g_0 g_1 + g_1 = 0 \\ g_0\, \theta(g_0) + g_1\, \theta(g_1) + 1 = 0 \end{cases}$$

i.e $g_1(g_0+1) = 0$ and $g_0^3 + g_1^3 = 1$. We get three polynomials X^2+1, $X^2+\alpha$ and $X^2+\alpha^2$. The bound of the polynomials $X^2+\alpha$ and $X^2+\alpha^2$ is X^4+X^2+1, so these two polynomials generate Hermitian self-dual central θ-codes which are not ideal θ-cyclic. One can notice that the remainder in the left division of X^4 by $X^2+\alpha$ (resp. $X^2+\alpha^2$) is equal to α^2 (resp. α). ■

The following lemma enables to give a more accurate description of Hermitian self-dual module θ-codes.

Lemma 1 *Let $\mathcal{C}$ be a Hermitian self-dual module θ-code with generator polynomial g of degree k and constant term $\neq 0$. Then*

- *there exists a non zero constant c and $h \in \mathbb{F}_q[X,\theta]$ such that $gh = X^{2k} - c = hg$;*
- *if k is even then $\theta(c)\, c = 1$; else $c^2 = 1$;*
- *if $\theta(c) \neq c$ then all odd terms of g cancel.*

PROOF. Let us assume that $\mathcal{C}$ is a Hermitian self-dual module θ-code of length $2k$ and let g be its generator polynomial. Then there exists c in $F - \{0\}$ and h in $\mathbb{F}_q[X,\theta]$ such that $gh = X^{2k} - c$. So $(gh)g = X^{2k}g - cg = gX^{2k} - cg$ because X^{2k} is in the center of $\mathbb{F}_q[X,\theta]$. We deduce from this that g divides cg on the left and as $g_0 \neq 0$, we get $gc = cg$. So $g(hg) = gX^{2k} - gc$ and $hg = X^{2k} - c$.
The polynomial g^H divides on the left $X^{2k} - \theta^{k+1}(1/c)$ and as the leading term $\theta^{k+1}(h_0)$ of g^H commutes with X^{2k}, the polynomial $1/\theta^{k+1}(h_0)g^H$ divides also $X^{2k} - \theta^{k+1}(1/c)$. Therefore g and $1/\theta^{k+1}(h_0)g^H$ are both monic and generate the same code, they must be equal. So $X^{2k} - c = X^{2k} - \theta^{k+1}(1/c)$ and if k is odd $c = 1/c$; if k is even, $c = \theta(1/c)$.
Lastly, as $gh = hg = X^{2k} - c$, we have $(X^{2k} - c)g = g(X^{2k} - c)$ so $\forall i \in \{0,\ldots,k\}, (c - \theta^i(c))\, g_i = 0$. For odd integers i, we get $(c - \theta(c))\, g_i = 0$. So if $\theta(c) \neq c$ then all odd terms of g cancel. ∎

The last point of this lemma implies that any Hermitian self-dual module θ-code which is not θ-constacylic (i.e. $\theta(c) \neq c$) has a generator polynomial which is quite "sparse". The minimum distances of these codes are worse than the minimum distances of the self dual θ-constacyclic codes previously obtained in [4]. This can be explained by the "sparsity" of this generator polynomial.

EXAMPLE. There are six Hermitian self-dual module θ-codes of length 20 over $\mathbb{F}_4$ which are central but not θ-cyclic. They give two non equivalent Hermitian self-dual module θ-codes over $\mathbb{F}_4$. The polynomial $X^{10} + \alpha^2$ divides on the left $X^{20} - \alpha$ and its bound is $X^{20} + X^{10} + 1$. It generates a $[20, 10, 2]_4$ Hermitian self-dual module θ-code which is θ-central and not θ-cyclic. The polynomial $X^{10} + \alpha\, X^8 + X^6 + \alpha\, X^4 + \alpha\, X^2 + \alpha^2$ also divides on the left $X^{20} - \alpha$ and its bound is $X^{20} + X^{18} + X^{16} + X^8 + X^6 + X^2 + 1$. It generates an $[20, 10, 4]_4$ Hermitian self-dual module θ-code which is θ-central and not θ-cyclic. The best distance for ideal θ-cyclic codes of the same length is 6 ([4]). One can notice the sparsity of these generator polynomials which may explain the bad distances of the codes they generate. ∎

References

[1] Berrick, A., Keating, M., 2000. An introduction to rings and modules. Cambridge Studies in Advanced Mathematics 65, Cambridge University Press.

[2] Bosma, W., Cannon, J., Playoust, C., 1997. The magma algebra system i: The user language. Journal of Symbolic Computation 24, 235–265.

[3] Boucher, D., Geiselmann, W. and Ulmer, F., *Skew Cyclic Codes*, Applied Algebra in Engineering, Communication and Computing, 18, 379-389 (2007)

[4] Boucher, D. and Ulmer, F., *Coding with skew polynomial rings*, Prépublication IRMAR 08-07, to appear in *Journal of Symbolic Computation*

[5] Chaussade, L., Loidreau P. and Ulmer, F., *Skew codes of prescribed distance or rank*, Designs, Codes and Cryptography, 50(3), 267-284 (2009)

[6] Gaborit, P., Otmani, A., 2002. Tables of Euclidian and Hermitian self-dual codes over $GF(4)$.

`http://www.unilim.fr/pages_perso/philippe.gaborit/SD/`

[7] McDonald, B. R., *Finite Rings with Identity*, Marcel Dekker Inc. (1974).

[8] Ore, O., Theory of non-commutative polynomials. *Ann. of Math.* **34**, (1933)